ZCASH FOUNDATION Q4 2022 REPORT

A review of Q4 2022 development, expenses and approved grants

The Zcash Foundation is a 501(c)(3) public charity that builds financial privacy infrastructure for the public good, primarily serving users of the Zcash protocol and blockchain.

March 2023

zfnd.org

CONTENTS

Did you know?

Zcash Community Grants (ZCG) has millions of dollars in funding available for projects that contribute to the growth of the Zcash ecosystem. Click here to learn more and to submit your grant request!

A WORD FROM ZF'S EXECUTIVE DIRECTOR

This is the Zcash Foundation's quarterly report for Q4 2022. Our goal with these reports is to provide a summary of the Foundation's activities, and an overview of our finances, including a detailed breakdown of our spending. We welcome feedback, so if you have any questions or suggestions, please post them to the Zcash Community forums!

The Engineering team tagged the first Zebra release candidate this quarter, and we have scheduled an audit of Zebra, which will begin in Q1 2023. Our next objective for Zebra is to add functionality to enable miners to use Zebra to generate block templates. The fact that we're adding this functionality to Zebra should not be construed as support for proof of work. The Foundation is supportive of moving away from proof of work to a more environmentally-friendly consensus mechanism, and it's likely that we'll still need to generate block templates, no matter what consensus mechanism we move to.

On the FROST front, the draft specification entered the last call for comments phase, while work continued on completing our reference implementation, including ticking off the remaining curves from the specification, and working on the distributed key generation protocol described in the FROST paper.

During Zcon, we announced plans to hire a community support coordinator to provide technical support to the Zcash ecosystem. In October, we hired Autotunafish to fill that role. Autotunafish is a long-standing member of the Zcash community, and already has a track record of assisting fellow community members with technical issues on the community forum.

continued on next page

A WORD FROM ZF'S EXECUTIVE DIRECTOR

In December, we welcomed J.W. Verret and Marta Belcher to the Zcash Foundation board, and bade farewell to Matt Green and Ian Miers, both of whom will continue to support the Foundation as members of our Technical Advisory Board.

The end of the year marked the end of four Zcash Community Grants committee members' terms (Adi, Jason McGee, Michael Harms and Wobbzz). Adi opted against seeking re-election in order to focus on his work with Nighthawk Apps, while the other three incumbents stood for re-election, alongside five other candidates. Jason, Michael and Wobbzz were duly re-elected by ZCAP for another term, along with new committee member Amber O'Hearn.

During this quarter, the committee approved seven grants, totalling over $875,000.

As the year drew to a close, the ZF team were busy planning Zcon 4, which will take place in Barcelona from July 30th to August 1st 2023. We are currently accepting proposals from potential speakers, panellists and workshop leaders, and we plan to open attendee registration in March.

We are also planning the first in what we hope will become a new series of hyper-local events called Zcon Voices. The first event is being led by the Zcash Brazil community, and will take place in Rio de Janeiro on March 18th. It will be delivered in Portugese and, therefore, is called Zcon Vozes.

Jack Gavigan
2nd March 2023

THE FUTURE OF ZCASH

At the Zcash Foundation, we believe that the success of Zcash and the principles it embodies relies on a positive feedback loop involving:

- **developers** who improve the Zcash protocol, and create the products, tools and services that support its use;
- **utility** that enhances the ability to use ZEC and the Zcash platform for a broader and more flexible range of purposes;
- broader **adoption** of Zcash as a platform for commerce, with ZEC as its native currency and;
- **users** who are attracted by the utility of ZEC and the services that entrepreneurs build on the Zcash platform.

Our strategic objectives are to:

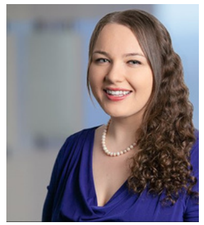
- **Support the Zcash community** - We do this by running Zcon, maintaining the community forums, and by giving the community a voice through the Zcash Community Advisory Panel.
- **Foster the growth of the Zcash ecosystem** - We aim to do this by removing obstacles that discourage developers, users, entrepreneurs and others from building, adopting or otherwise supporting Zcash.
- **Make Zcash smarter** - We believe that programmability is a key mechanism for enhancing Zcash's utility. In time, we will explore options for achieving this.

ZF APPOINTS TWO NEW BOARD MEMBERS

We are pleased to announce that J.W. Verret and Marta Belcher have joined the board of the Zcash Foundation.

J.W. and Marta bring a wealth of experience and expertise, which will benefit the Zcash Foundation as it continues to grow and evolve, and help the Foundation better serve the Zcash community.

J.W. Verret is an Associate Professor at the Antonin Scalia Law School at George Mason University, where he teaches banking, securities, and corporation law. Jay previously spent two years as Chief Economist and Senior Counsel for the U.S. House Committee on Financial Services, and he served on the SEC's Investor Advisory Committee.



Marta Belcher is President and Chair of the Filecoin Foundation as well as the Filecoin Foundation for the Decentralized Web. She is also General Counsel and Head of Policy at Protocol Labs, and special counsel to the Electronic Frontier Foundation.

THANK YOU MATT AND IAN

J.W. and Marta’s arrival coincides with Matt Green and Ian Miers’ departure from the ZF board.

On behalf of the board, and the Zcash community as a whole, we express our heartfelt gratitude to Matt and Ian, for the guidance, advice and feedback they have provided during their time on the board; for their historical contributions that were instrumental in the creation of Zcash and its growth, development and evolution to where it is today; and for their ongoing contributions as members of the Technical Advisory Board.

Read the full announcement here.

Q4 SCIENCE & ENGINEERING SUMMARY

During the final quarter of 2022, the Engineering team tagged the first stable release candidate, marking the first version of the Zebra zcash node implementation which the Foundation is happy to have audited and ready for stable release. We also started working towards implementing functionality to allow Zebra to generate blocks for mining.

Work on the FROST specification reached its conclusion at version 11 with the team asking the CFRG chairs to initiate a last call for comments to decide on its publication. In parallel, work on the FROST reference implementation was also completed to support all of the curves listed in the specification.

During this quarter we also started looking into Oblivious Message Retrieval as a potential way to improve wallet performance, as well as evaluating it as a potential solution to the privacy leaks when using lightwalletd.

Q4 SPRINTS

Sprint 20: During this sprint the engineering team finished off the last outstanding issues related to lightwalletd support and tagged the first release candidate of zebra: Zebra 1.0.0-rc.0. With this release we are confident that Zebra's consensus rules, node sync, and lightwalletd RPCs are ready for user testing and experimental use ahead of a full audit.

The team also continued working on v08 of the FROST specification and updated the reference implementation accordingly.

Sprint 21: The team started working on implementing support to enable mining pools to be able to use zebrad to generate a block template for mining, and broadcast a newly-mined block to the Zcash network, starting with support for getblockhash and getblockcount RPC calls. We also made some fixes to the mempool in order to provide more accurate transaction information to support mining RPCs. During this sprint we also added block writing metrics

On FROST, the team worked on implementing Distributed Key Generation (DKG.)

Sprint 22: During this sprint the team released the second release candidate: Zebra 1.0.0-rc.1, removing some outdated dependencies and unused code to make a few final improvements before sending Zebra for audit. The team also continued working on mining RPC methods to support mining pools, mostly centered around the getblocktemplate RPC call and also the submitblock call.

We also started looking into OMR as a potential solution to some privacy leaks when using lightwalletd.

Work on FROST continued with updates to make the reference implementation conformant with v11 of the specification and adding support for Ed25519 curve. The team also made updates to the re-randomizable FROST implementation to bring it up to date with v11 of the specification.

continued on next page

Q4 SPRINTS

Sprint 23: After a period of struggling with CI, we finally solved some issues we were having when running tests on GCP infrastructure that were impacting PRs getting merged to our main branch. We continued working on the getblocktemplate RPC call and improving on transaction selection from the mempool.

On FROST, the team reached out to various people to ask them for their comments and support of the draft as the last call for comments on the FROST draft specification was kicked off. This is a key step in deciding whether the FROST specification is ready for publication.

Sprint 24: In this sprint, as well as continuing work on the getblocktemplate RPC call, we also worked on implementing ZIP-317 rules to evict transactions from Zebra's mempool.

On FROST, we finished implementing FROST on all of the required curves, bringing the reference implementation up to date with the spec.

Sprint 25: Sprint 25 was the last sprint of 2023 with the team focused on finishing off the functionality required to generate valid blocks for mining as well as any other mining related functionality and RPCs. One notable improvement is that we are now re-verifying mempool transactions after a chain fork, rather than re-downloading them all. This should be faster and put less load on the Zcash network.

During this sprint we also tagged Zebra 1.0.0-rc.2. The team also made some updates to Zebra to support the latest version of ZIP-317 which should help to prevent spam transactions on the Zcash network.

On FROST, we continued polishing the reference implementation, improving testing coverage and running benchmarks to test performance and identify possible optimizations. Some minor editorial updates to the specification were also made in response to comments received after the last call for comments was issued.

Q4
FROST NEWS

Improving upon the state of the art in threshold signature protocols

FROST stands for Flexible Round-Optimized Schnorr Threshold. It is a threshold signature scheme that essentially reduces network overhead during signing operations while employing novel techniques to protect against forgery attacks applicable to similar schemes.

IETF Last Call!

We entered the CFRG's working group last call for the FROST IETF draft and are currently in the process of opening pull requests to address the feedback that we received. The overall community response has been very positive and we expect to be finalizing the IETF draft in early 2023. More work is being performed on the re-randomized variant of FROST to ensure unlinkability on the Zcash blockchain; we are moving towards having a ZIP and corresponding security analysis also in 2023.

DID YOU KNOW?

5%

- The Zcash Community created the Dev Fund in late 2020 as a means of funding ongoing development of the Zcash protocol by the Zcash Foundation (5% of the block reward), the Electric Coin Company (7%), and the Zcash Community Grants program (8%).

- Annually, the Zcash Foundation receives approximately 65,745 ZEC from the Dev Fund.

- In addition, the Foundation receives 105,192 ZEC as a restricted donation, which may only be disbursed as major grants.

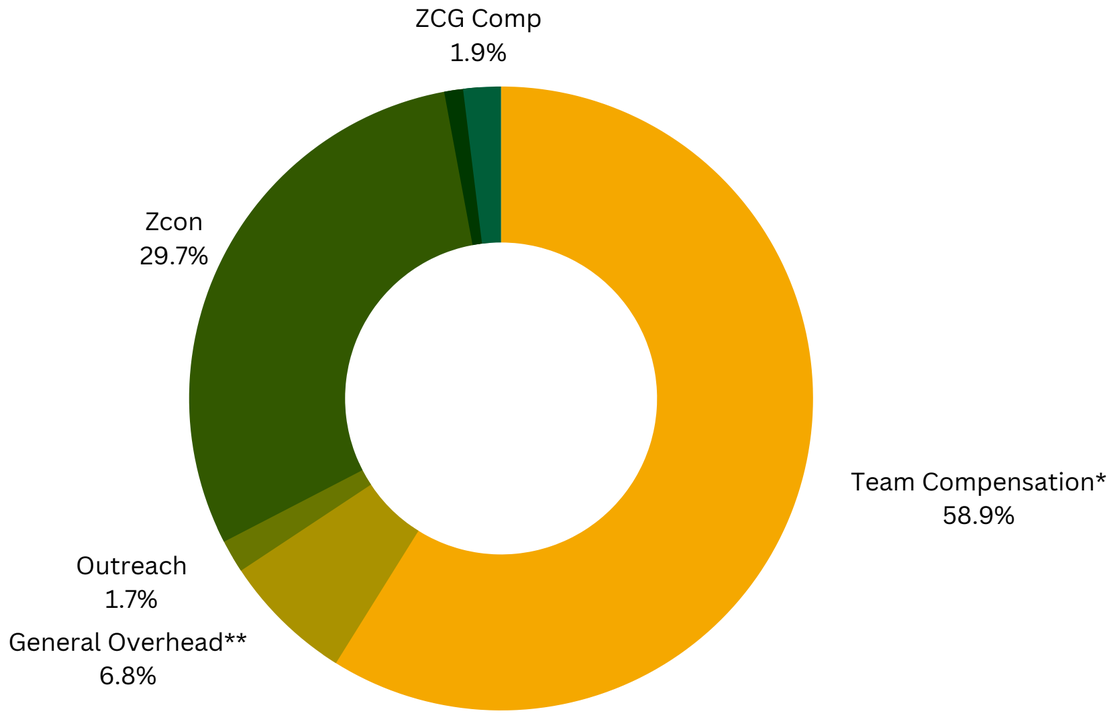
Q4 ZF FINANCIALS

The USD value of funds received and held by ZF during Q4 was calculated using the following Messari closing prices for December 31:	ZF funds received in Q4 2022:	Total held at end of Q4 2022:
• $37.36 USD/ZEC • $1,195.48 USD/ETH • $16,535.66 USD/BTC	Received 16,489 ZEC ($616,029 USD) at an average of 5,496 ZEC ($205,331 USD) a month and realized approximately $308,183 USD per month in operating expenses.	$4,673,977 USD, 192,217 ZEC, 66 BTC, and 12 ETH for a total value of $12,958,572 USD and held custody of 150,803 ZEC, 60,000 USDC, and $2,368,198 USD for a total value of $8,062,186 USD restricted for use in funding major grants as selected by ZCG & the ZCG discretionary fund.

Q4 ZF USE OF FUNDS

During Q4 2022, ZF's operating expenses averaged approximately $415,826 USD per month. The breakdown of resource allocation is as follows:

Team Compensation	$608,327
General Overhead	$108,132
Outreach	$5,337
Zcon/Zcon Voices	$14,616
Conference Attendance & Team Building	$5,639
ZF Grants	$160,000
ZCG Member Compensation	$22,500
Total	**$924,550**



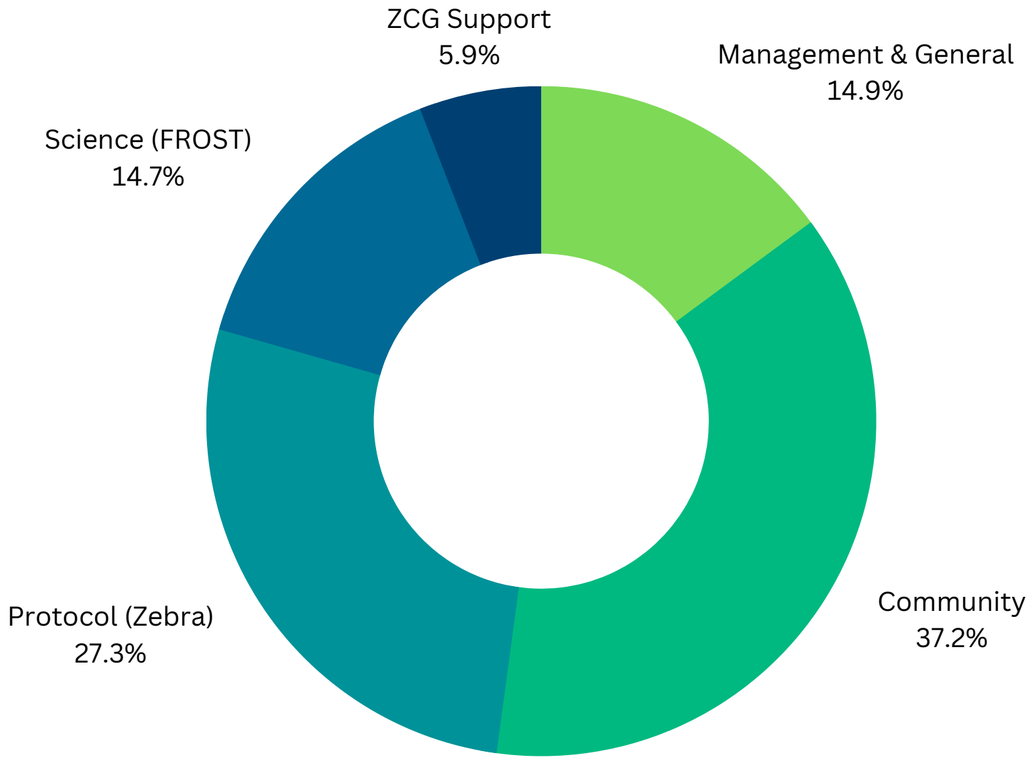
*Team compensation encompassed all compensation and benefits paid to ZF staff and contractors. ZF does not operate any form of retention bonus or deferred compensation scheme.

**General overhead refer to costs not related to labor. These include: accounting, HR account fees, custodial service and banking fees, grant platform maintenance, insurance, legal fees, and trademark enforcement.

Q4 ZF PROGRAMS

The following table and chart explain what type of programs ZF invested in during Q4. Please note, each ZF team member's compensation and benefits are allocated to the program(s) they contribute to.

Management & General	$153,801
Community	$95,236
Protocol (Zebra)	$297,724
Science (FROST)	$129,474
ZF Grants	$160,000
ZCG Support	$88,316
Total	$924,550



Q4 ZF FINANCIAL SNAPSHOT

	UNRESTRICTED FUNDS		RESTRICTED FUNDS - ZCG	
LIQUID ASSETS	**COIN BALANCE**	**USD VALUE**	**COIN BALANCE**	**USD VALUE**
USD	$ -	$4,673,977	$ -	$2,368.198
USDC	$ -	$ -	60,000	$60,000
ZEC	192,217.37	$7,181,241	150,802.67	$5,633,988
BTC	65.87	$1,089,135	$ -	$ -
ETH	11.89	$14,220	$ -	$ -
		$12,958,572		**$8,062,186**
LIABILITIES				
GRANT COMMITMENTS		$102,580		$2,645,925
ACCRUED EXPENSES & PAYROLL LIABILITIES		61,105		$ -
TOTAL LIABILITIES		163,685		2,645,925
NET LIQUID ASSETS		**$12,794,887**		**$5,416,261**

USD VALUE (as of December 31) : $37.36 USD/ZEC | $16,535.66 USD/BTC | $1,195.48 USD/ETH

NB: This simplified balance sheet does not include intangible or illiquid assets and liabilities that would appear on ZF's full balance sheet (e.g. trademark, etc.).

ZCG KEY FINANCIALS

Zcash Community Grants - Q4 2022

The USD value of funds received and held by ZF on behalf of ZCG during Q4 were calculated using the following Messari closing price for Dec. 31:

- $37.36 USD/ZEC

Restricted funds received by ZF in Q4 2022:

- The Foundation received 26,382 ZEC ($985,632 USD) at an average of 8,794 ZEC ($328,544 USD) a month of ZCG restricted funds.
- The Foundation distributed 17,118 ZEC and $47,124 USD (valued at $980,607 USD at time of payment) in Quarter 4 of ZCG restricted funds for grants approved by the ZCG committee and 702 ZEC (valued at $33,192 USD at time of distribution) from the ZCG discretionary fund.

Total restricted funds held by ZF on behalf of ZCG at the end of Q4:

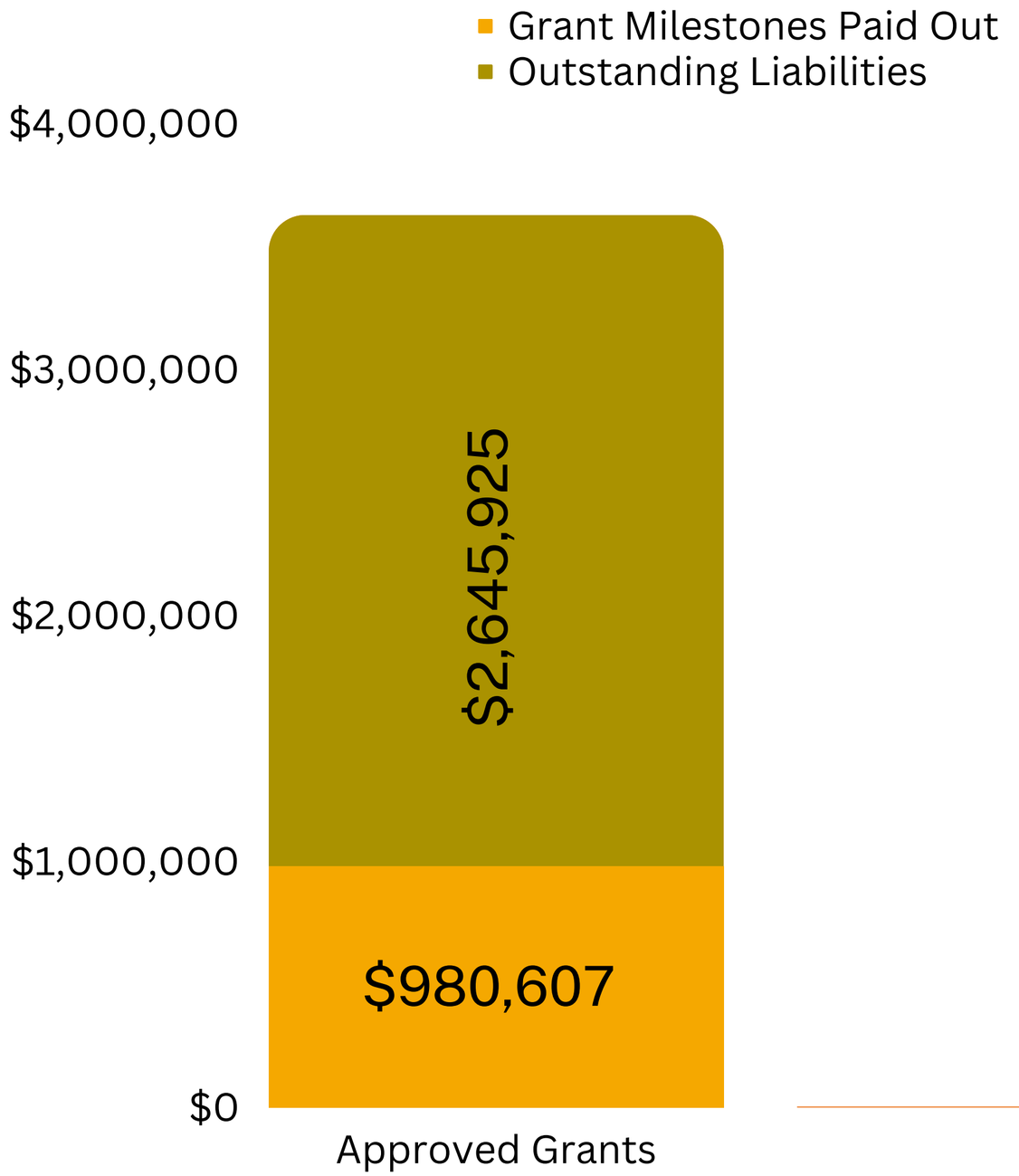
- ZEC = 150,803
- USD = $2,368,198
- USDC = 60,000

Total = $8,062,198

Q4 ZCG GRANTS

The Zcash Community Grants Program (ZCG) provides individuals and teams access to funding so they can contribute to the growth of the Zcash ecosystem. Some key areas of funding include: core infrastructure, wallets, interoperability, apps, ongoing services, integrations, research, and community. During Q4, ZCG approved 7 grants totaling $876,314 USD.

- Of the newly approved grants, ZCG paid out $205,080 USD for initial payments and milestones.
- ZCG also paid out $775,527 for grants approved in previous quarters.
- At close of Q4 2022, ZCG had outstanding grant liabilities of $2,645,925 for approved grants.



ZCG METRICS YTD

ZCG Website

ZCG Dashboard

21

grants approved YTD

57

grants reviewed YTD

18

open grants

21

days proposal submission to decision

9

% of discretionary budget used YTD

11

ambassadors

ZCG Q4 APPROVED GRANTS

		CRYPTO MONDAYS DAO				EIGER
ToDeFi: Torino Decentralized Finance Conference Conference sponsorship Link to Grant	**Orchard and UA for Ywallet** Add Orchard features to Ywallet Mobile and Desktop Apps Link to Grant	**CryptoMondays** Leverage 70+ global chapters to spread awareness about Zcash and the importance of privacy in general Link to Grant	**The Zcash Podcast on the Digital Cash Network** Monthly Zcash podcast highlighting news and updates Link to Grant	**Ziggurat 3.0** Expands Ziggurat's coverage by outfitting the crawler with advanced telemetry. Link to Grant	**Zcash Brazil 2023** Funding to expand Zcash's presence in Brazil in 2023. Link to Grant	**Equilibrium** An SDK to use native Rust Zcash libraries in other languages (Ruby, Kotlin, Python, and Swift) Link to Grant

ZCASH AMBASSADORS

Zcash Community Grants

- Eric Vaughn - US
- Jacob Feldman - US
- Madison Parks - US
- Yoditar - Venezuela
- Michae2xl - Brazil
- Chidi - Nigeria
- Zoz - Saudi Arabia
- artkor - Russia
- Mucu - Uganda NEW
- Aiden - South Korea
- Laika - Germany NEW

Click here to learn more about the Zcash Ambassador program

THANK YOU ZF BOARD!

ZF would like to thank our board members for their continued contributions. Board members are uncompensated volunteers, dedicating their time and expertise to shape the future of the Zcash Foundation while providing vital governance oversight.

- **Jack Gavigan**: Executive Director of the Zcash Foundation.
- **Andrew Miller** (Chair & Treasurer): Assistant professor in the electrical and computer engineering department at the University of Illinois at Urbana-Champaign, and an associate director of the Initiative for Cryptocurrencies and Contracts.
- **Peter Van Valkenburgh**: Director of Research at Coin Center, a nonprofit organization focused on research, education, and advocacy at the intersection of policy and cryptocurrencies.
- **Amber Baldet**: CEO of Clovyr, former J.P. Morgan blockchain program lead, and co-creator of a zero-knowledge settlement layer for enterprise Ethereum.
- **Marta Belcher**: President and Chair of the Filecoin Foundation as well as the Filecoin Foundation for the Decentralized Web. She is also General Counsel and Head of Policy at Protocol Labs, and special counsel to the Electronic Frontier Foundation.
- **J.W. Verret**: Associate Professor at the Antonin Scalia Law School at George Mason University, where he teaches banking, securities, and corporation law.